CLAIMS:

1.   A method of controlling authentication of a first device to a second device, the devices being assigned respective device identifiers, the method comprising distributing to the first device a group certificate identifying a range of non-revoked device identifiers, said range encompassing the device identifier of the first device.

5

2.   The method of claim 1, in which the respective device identifiers correspond to leaf nodes in a hierarchically ordered tree, the method further comprising identifying in the group certificate a node in the hierarchically ordered tree, said node representing a subtree in which the leaf nodes correspond to the range of non-revoked device identifiers.

10

3.   The method of claim 2, further comprising identifying in the group certificate a further node in the subtree, said further node representing a further subtree in which the leaf nodes correspond to device identifiers excluded from the range of non-revoked device identifiers.

15

4.   The method of claim 1, in which the respective device identifiers are selected from a sequentially ordered range, the method further comprising identifying in the group certificate a subrange of the sequentially ordered range, said subrange encompassing the range of non-revoked device identifiers.

20

5.   The method of claim 1, further comprising identifying plural respective ranges of non-revoked device identifiers in a single group certificate.

6.   The method of claim 5, in which the plural respective ranges in the single group certificate are sequentially ordered, the method further comprising identifying the plural respective ranges in the single group certificate through an indication of the lowest and highest respective ranges in the sequential ordering.

25

7. The method of claim 1, in which the group certificate comprises an indication of a validity period.

8. The method of claim 1, in which the group certificate comprises a version indication.